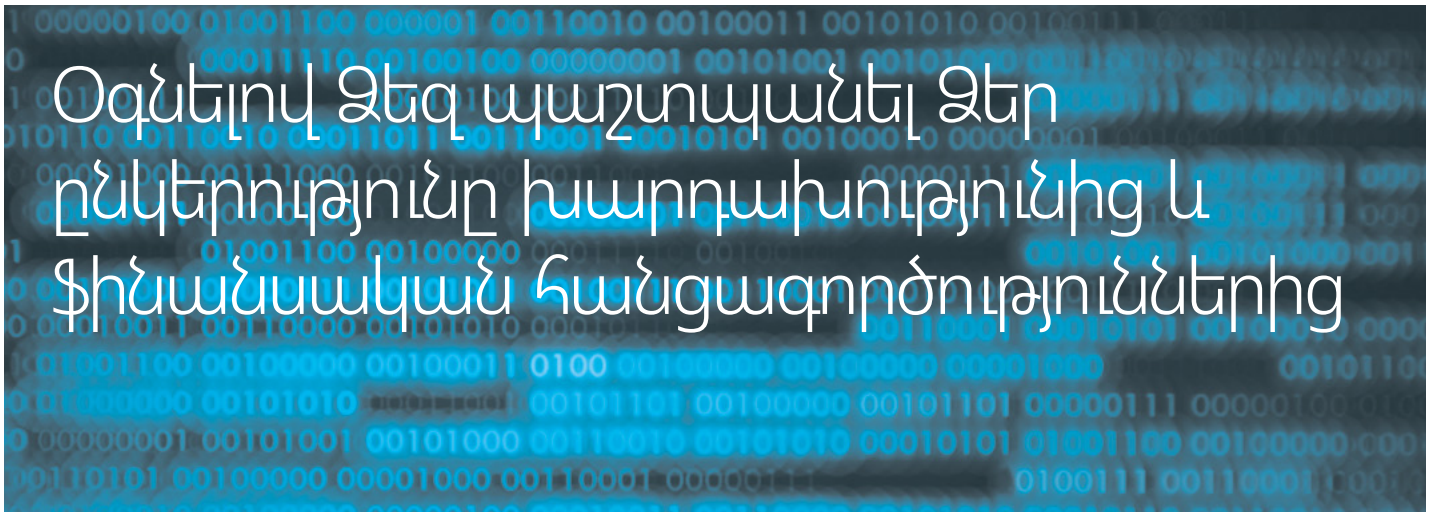

Օգնելով Ձեզ պաշտպանել Ձեր ընկերությունը խարդախությունից և ֆինանսական հանցագործություններից

HSBC-ն լուրջ ուշադրություն է դարձնում զեղծարարությանը և ֆինանսական հանցագործություններին: Չնայած նրան, որ զեղծարարության բացահայտման նպատակով մենք գործածում ենք առաջատար համակարգեր, այնուամենայնիվ, ցանկանում ենք Ձեզ տեղեկացնել այն եղանակների մասին, որոնց միջոցով զեղծարարները փորձում են գողանալ ոչ միայն Ձեր գումարը, այլ նաև Ձեր ընկերության ինքնությունը:

Ստորև ներկայացված են որոշ խորհուրդներ՝ ինչպես չդառնալ զեղծարարության զոհ: Խնդրում ենք ծանոթանալ նաև Իրավաբանական անձանց «Հիմնական պայմաններին»:

Բիզնես էլ. հաղորդագրության միջոցով զեղծարարություն
Այս զեղծարարության տեսակը թիրախավորում է օտարերկրյա մատակարարների և/կամ գործարարների հետ աշխատող կազմակերպությունների, որոնք հաճախ են իրականացնում վճարումներ ընկերության սեփականատիրոջ, տնօրենի կամ ֆինանսական տնօրենի անունից:

Առկա է այս զեղծարարության երկու հիմնական տեսակ՝

- Էլ. փոստի սփուֆինգ **(spoofing)**՝ սա ենթադրում է էլ.փոստի միջոցով մանիպուլյացիա, երբ զեղծարարի էլ.փոստը նմանացվում է այլ իրական էլ. փոստի հասցեին :
- Այս միջոցով զեղծարարները կեղծում են իրական մատակարարների էլ.փոստի հասցեն՝ կեղծ տվյալներով հաշիվ-ապրանքագիր ներկայացնելով: Այս դեպքում իրական մատակարարի էլ. փոստի հասցեն չի կոտրվում, այլ փոխարենը ստեղծվում է իրական մատակարարի դոմեյնին նման հասցե, ինչը շատ մարդիկ չեն նկատում, ինչպես օրինակ՝ @CompanyACB.com՝ @CompanyABC.com-ի փոխարեն:
- Էլ. փոստի կոտրում: Զեղծարարության այս տեսակը հանդիսանում է կազմակերպության ղեկավար անձի, օրինակ՝ ֆինանսական տնօրենի, էլ.փոստի հասցեից զեղծարարություն. զեղծարարը կոտրված էլ.փոստի հասցեից կեղծ վճարման հրահանգ է ուղարկում մեկ այլ՝ հաճախ կրտսեր աշխատակցին:

Ուշադրություն:

1. Համոզվեք, որ Ձեր աշխատակիցները գիտեն համապատասխան քայլերի հաջորդականությունը՝ պարզելու վճարման հարցումն ուղարկած էլ.փոստի իսկությունը:

2. Այս տեսակի զեղծարարության զոհ չդառնալու նպատակով մշտապես ստուգեք Ձեր ընկերության վճարում իրականացնող վերահսկողության համակարգերը:

Վճարման շեղում / հաշիվ-ապրանքագրի կեղծում
Զեղծարարության այս տեսակը ենթադրում է, որ զեղծարարը խարդախությամբ դրդում է ընկերությանը փոխելու վճարման ստացողի բանկային հաշվեհամարը: Զեղծարարները հանդես են գալիս ընկերության մշտական մատակարարի անունից և տրամադրում իբրև փոփոխված բանկային հաշվեհամարի մանրամասները:

Սա ներառում է

- հաճախորդների շինծու տվյալների և բանկային հաշիվների ստեղծում՝ կեղծ վճարումներ կատարելու նպատակով:

Ինչպե՞ս նվազեցնել Ձեր ընկերության՝ հաշիվ-ապրանքագրի կեղծման զոհ դառնալու հավանականությունը

- Համոզվեք, որ այն աշխատակիցները, որոնք ներգրավված են հաշիվ-ապրանքագրերի և դրանց հիմնական տվյալների փոփոխության գործընթացում, տեղեկացված են զեղծարարության հավանական վտանգների վերաբերյալ:
- Միշտ վավերացրեք ֆինանսական պայմանավորվածության ցանկացած փոփոխություն մատակարարի հետ՝ օգտագործելով Ձեզ մոտ գրանցված կոնտակտային տվյալները:

HSBC

Ֆիշինգ
Սա ենթադրում է էլ.հասցեին ուղարկված նամակներ, որոնք ուղղորդում են մարդկանց դեպի այլ վեբ կայքեր, որտեղ նրանք թողնում են անձնական կամ ֆինանսական գաղտնի տեղեկատվություն: Թեև այս էլ.նամակները կարող են թվալ օրինական կայքերից ուղարկված, այնուամենայնիվ, դրանց նպատակն է գողանալ Ձեր անձնական տեղեկատվությունը՝ Ձեր հաշիվներ մուտք գործելու նպատակով: Այս գործընթացը հայտնի է որպես ֆիշինգ: Մի՛ պատասխանեք այն նամակներին և մի հետևեք էլ. նամակում ներառված հղմանը, որտեղ, օրինակ զգուշացվում է, որ Ձեր հաշիվը կսառեցվի եթե Դուք չհաստատեք Ձեր անձնական տեղեկատվությունը: Փոխարենը՝ Դուք կարող եք կապ հաստատել ընկերության հետ Ձեզ արդեն ծանոթ հեռախոսահամարով:
Ջնջեք նմանատիպ էլ. նամակները:

Վիշինգ
Ձեղծարարը զանգահարում է ընկերություն՝ ներկայանալով որպես բանկի աշխատակից, ոստիկան, մատակարար, հաճախորդ կամ այլ վստահություն ներշնչող անձ: Սովորաբար հեռախոսազանգի նպատակն է զոհին դրդել հետևյալ գործողությունների՝

- Տեղափոխել գումարն այլ հաշվի՝ իբրև ապահովության կամ պահպանման համար
- Կանխիկացնել գումարը և փոխանցել այն զեղծարարին՝ հետաքննության նպատակով
- Տրամադրել անձնական տեղեկատվություն, որը թույլ կտա մուտք գործել Ձեր ընկերության բանկային հաշվին:

Ուշադրություն:
1.Ուշադիր եղեք անծանոթ զանգերին, հատկապես երբ Ձեզանից կպահանջվի տրամադրել գաղտնի տեղեկատվություն ընկերության մասին:

2.Եթե կասկածներ ունեք, մի վախեցեք դադարեցնել հեռախոսազանգը՝ հրաժարվելով տրամադրել որևէ տեղեկատվություն:

3.Խոսակցությունը պետք է ավարտվի երկուստեք, այսպիսով, համոզված եղեք, որ Ձեզ զանգահարողը ևս ավարտել է զանգը, և դուք կարող եք օգտագործել մեկ այլ հեռախոսահամար՝ պարզելու զանգահարողի իսկությունը:

4.Ձեղծարարները կարող են միտումնավոր կեղծել հեռախոսի էկրանին ցուցադրվող համարը՝ փորձելով այն ներկայացնել որպես բանկի իսկական հեռախոսահամար:

5.HSBC-ին Ձեզանից երբեք չի պահանջի գեներացնել անվտանգության կոդը՝ սեղմելով դեղին կոճակը կամ խնդրելով Ձեզ տրամադրել Ձեր PIN համարը:

6.Երբեք մի՛ փոխանցեք ընկերության անվտանգությանը վերաբերող տեղեկատվությունն այլ անձանց: Շատ կարևոր է պահպանել Ձեր հաշիվը և անվտանգության տեղեկատվությունն ապահով:

Հանցագործները կարող են տիրապետել Ձեր ընկերության մասին հիմնական տեղեկատվությանը՝ անուն, հասցե, հաշվեհամարի տվյալներ: Մի՛ ենթադրեք, որ զանգահարողը վստահելի անձ է, այն պատճառով, որ տիրապետում է այդ տեղեկատվությանը կամ ներկայանում է որպես իրական կազմակերպություն:

Կեղծ չեկ
Այս զեղծարարությունը ենթադրում է Ձեր բանկային հաշվից դուրս գրված չեկերի կեղծում կամ ապօրինի փոփոխում: Ստորև ներկայացված են զեղծարարության զոհ չդառնալու որոշ խորհուրդներ

- Ստուգեք Ձեր չեկերը: Ավելացրեք հավելյալ տեղեկատվություն՝ ինչպես օրինակ հաշվին կցված այլ համար:
- Ամբողջությամբ օգտագործեք Ձեր ստորագրությունը չեկերի վրա, ոչ միայն պարզապես սկզբնատառերը:
- Ստուգեք չեկերը քաղվածքների հետ: Տեղեկացրեք մեզ ցանկացած անհամապատասխանության դեպքում:
- Պահեք դատարկ չեկերն ապահով վայրում:

Պաշտպանեք Ձեր քարտը:
- Ստորագրեք և ակտիվացրեք Ձեր քարտը ստանալու պահին:
- Դուք կարող եք ակտիվացնել Ձեր քարտն օնլայն բանկինգի միջոցով, զանգահարելով մեզ ստորև նշված հեռախոսահամարներով կամ օգտագործելով HSBC ATM-ը:
- Զանգահարեք մեզ ստորև նշված հեռախոսահամարներով, եթե Ձեր՝ ժամկետանց հին քարտին փոխարինող նոր քարտը չի ժամանել հին քարտի վավերականության ժամկետի ավարտից մեկ շաբաթ առաջ:

Պաշտպանեք Ձեր PIN-ը
- Երբեք մի պահպանեք Ձեր PIN-ը կամ անվտանգության այլ մանրամասներն այնպիսի վայրում, որը հասանելի է այլ անձանց:
- Ոչնչացրեք Ձեր PIN-ի մասին տեղեկատվությունը:
- Ընտրեք այնպիսի PIN, որը չի ասոցացվի Ձեր հետ և չի հանդիսանա թվերի հաջորդականություն՝ 1234 կամ 1111: Լավագույն տարբերակն է թվերի խառը հաջորդականության ընտրությունը կամ այնպիսի հաջորդականություն, որը Դուք կարևորում եք:.

Պահպանեք Ձեզ՝ գտնվելով ATM-ին մոտ
- ATM-ին կարող է հարմարեցված լինի սարք, որը կարող է օգնել զեղծարարին գողանալու քարտը կամ դրա տեղեկատվությունը: Եթե դուք նկատեք տարօրինակ սարք, կցված ATM-ին, մի փորձեք այն հեռացնել: Հեռու գնացեք ATM-ից և զանգահարեք հաճախորդների սպասարկման կենտրոն կամ ոստիկանություն:
- Միշտ մոտ կանգնեք ATM-ին և ձեռքով փակեք այն հատվածը, որտեղ հավաքում եք PIN-ը: Հանցագործները կարող են հետևել Ձեզ այն պահին, երբ դուք մուտքագրում եք PIN-ը մինչ փորձելը գողանալ Ձեր քարտը:
- Եթե ATM-ը չի վերադարձնում Ձեր քարտը, մի փորձեք մուտքագրել այն կրկին: Տեղեկացրեք մեզ՝ զանգահարելով հաճախորդների սպասարկման կենտրոն:

Պահպանեք Ձեր ընկերության քարտերը հեռախոսի միջոցով
- Երբ կատարում եք քարտային վճարումներ հեռախոսի միջոցով, քարտը պետք է լինի Ձեր առջև, քանի որ Ձեզանից կպահանջվի քարտի ժամկետի ավարտը, թողարկման ամսաթիվը և երեք նիշը, որը գրված է ստորագրության կողքին: Երբեք մի փոխանցեք Ձեր PIN-ը հեռախոսով, նույնիսկ եթե պահանջվի:
- Փորձեք չտրամադրել Ձեր քարտի մասին տեղեկատվությունը հանրային վայրերում, քանի որ այն կարող է լսելի դառնալ:
- Պահանջեք գործարքի փոստային կամ էլեկտրոնային հաստատում:

Եղեք պաշտպանված, երբ ինքներդ եք օգտագործում քարտը:

- PIN-ը մուտքագրելիս ձեռքով փակեք այն:
- Եթե կբախվեք դժվարությունների քարտն օգտագործելիս, ապա զանգահարեք հաճախորդների սպասարկման կենտրոն:
- Խնդրում ենք պահպանել Ձեր քարտերն ապահով վայրում:

Պաշտպանեք Ձեզ օնլայն հարթակներում

- Կատարեք գնումներ անվտանգության համակարգ ունեցող կայքերից՝ համոզված լինելով, որ անվտագության բանալին երևում է վեբ կայքի պատուհանում՝ անձնական տեղեկատվություն մուտքագրելիս: Ստորև ներկայացված է առավել մանրամասն տեղեկատվություն՝ ինչպես պաշտպանել Ձեզ օնլայն հարթակներում:
- Պահպանեք Ձեր պատվերի հաստատման պատճենը: Փոստային հասցեն և հեռախոսահամարը պետք է նույնպես առկա լինեն:
- Կրեդիտ քարտով օնլայն գնումներ կատարելիս, միշտ մուտք գործեք Mastercard Securecode կամ Verified by Visa համակարգերով: Վերջիններս ապահովում են անձնական տվյալների պաշտպանություն:

Պաշտպանեք Ձեր գաղտնաբառերը

- Օգտագործեք տարբեր գաղտնաբառեր տարբեր համակարգերի համար
- Մի օգտագործեք այնպիսի գաղտնաբառեր, որոնք կարող են կռահելի դառնալ, ինչպես օրինակ՝ երեխաների անունները կամ ծննդյան ամսաթվերը:
- Երբեք գրի մի առեք Ձեր գաղնաբառերը, սակայն երբ չունեք այլընտրանք, ապա պահպանեք դրանք այնպես, որպեսզի այլ մարդիկ այն չկռահեն:
- Որպես գաղտնաբառի հիշեցում մայրիկի անունն օգտագործելու փոխարեն, կարող եք ընտրել Ձեր սիրված մուլտ հերոսին կամ այլ հորինված կերպարի:
- Ձեր գաղտնաբառն ուժեղացնելու համար, օգտագործեք մեծատառեր/փոքրատառեր, ինչպես նաև թվեր:

...պաշտպանելով Ձեզ և Ձեր բիզնեսը

Ինքնության կեղծում

Օգտագործելով տարբեր եղանակներ՝ զեղծարարները կարող են տիրապետել այնպիսի անձնական տվյալների, ինչպիսիք են՝ կրեդիտ քարտի համարը, նրա ժամկետի ավարտը, Ձեր ծննդյան ամսաթիվը կամ Ձեր մայրիկի օրիորդական ազգանունը և այլն: Այս տեղեկատվությունը կարող է պահանջվել բանկային նոր հաշիվ բացելու կամ վարկի դիմելու համար:

Նվազեցրեք ռիսկը՝ հետևելով այս երեք հիմնական կետերի՝

- Ոչնչացրեք բոլոր տեղեկանքները, որոնք պարունակում են Ձեր բիզնեսի անվանումը, հասցեն կամ անձնական տեղեկատվություն:
- Ակտիվացրեք հեռախոսի անվտանգության համարը, քանի որ այն մեզ համար հանդիսանում է Ձեզ իդենտիֆիկացնելու անվտանգ եղանակ:
- Մի փոխանցեք հեռախոսի անվտանգության համարն այլ անձի, ով կապ է հաստատում Ձեզ հետ: HSBC-ն Ձեզանից երբեք չի պահանջի տրամադրել հեռախոսի անվտանգության համարը, երբ մենք ենք զանգահարում Ձեզ:

Եթե Ձեր ընկերությունը դարձել է զեղծարարության զոհ, տեղեկացրեք մեզ ստորև նշված հեռախոսահամարով կամ կորպորատիվ բիզնեսի զարգացման գծով կառավարչի միջոցով: